Algebraic analysis of quantum search with pure and mixed states

Daniel Shapira, Yishai Shimoni, and Ofer Biham
Racah Institute of Physics, The Hebrew University, Jerusalem 91904, Israel

An algebraic analysis of Grover's quantum search algorithm is presented for the case in which the initial state is an arbitrary pure quantum state $|\psi\rangle$ of n qubits. This approach reveals the geometrical structure of the quantum search process, which turns out to be confined to a four-dimensional subspace of the Hilbert space. It unifies and generalizes earlier results on the time evolution of the amplitudes during the search, the optimal number of iterations and the success probability. Furthermore, it enables a direct generalization to the case in which the initial state is a mixed state, providing an exact formula for the success probability.

PACS numbers: PACS: 03.67.Lx, 89.70.+c

I. INTRODUCTION

Grover's quantum search algorithm [1, 2] exemplifies the potential speed-up offered by quantum computers. It also provides a laboratory for the analysis of quantum algorithms and their implementation. The problem addressed by Grover's algorithm can be viewed as trying to find a marked element in an unsorted database of size N. While a classical computer would need, on average, $N/2$ database queries (and N queries in the worst case) to solve this problem, a quantum computer using Grover's algorithm, would accomplish the same task using merely $O(\sqrt{N})$ queries. This proves the enhanced power of quantum computers compared to classical ones for a whole class of oracle-based problems, for which the bound on the efficiency of classical algorithms is known. Moreover, it was shown [3] that Grover's algorithm is as efficient as theoretically possible [4]. A variety of applications were developed, in which the algorithm is used in the solution of other problems [5, 6, 7, 8, 9, 10, 11].

Several generalizations of Grover's original algorithm have been developed. The case in which there are several marked states was studied in Refs. [12, 13]. It was shown that when there are r marked states, Grover's algorithm can find one of them after $T = O(\sqrt{N/r})$ queries. A further generalization was obtained by allowing the replacement of the Hadamard transform, used in the original setting, by an arbitrary (but constant) unitary transformation [14, 15, 16], as well as by the replacement of the π inversion by an arbitrary (but constant) phase rotation [17, 18]. Another generalization was obtained by allowing the replacement of the uniform superposition of all basis states, used as the initial state of the algorithm in the original setting, by an arbitrary pure [19, 20] or mixed [21] quantum state. It was shown that the optimal time to perform the measurement that concludes the operation of the algorithm is independent of the initial state. However, the probability of success, $P_{\rm s}$, is reduced, and its value depends on the initial state. An explicit expression for P_s in terms of the amplitudes of the initial state was found [22]. This generalization provides an operational measure of entanglement of pure multi-partite quantum states [23, 24, 25].

In this paper we introduce an algebraic approach to the analysis of Grover's quantum search algorithm with an arbitrary initial quantum state. This approach reveals the geometrical structure of the search process, which turns out to be confined to a four dimensional subspace of the Hilbert space. This approach unifies and generalizes earlier results on the time evolution of the amplitudes during the search, the optimal number of iterations and the success probability. Furthermore, it enables a direct generalization to the case in which the initial state is a mixed state, providing an exact formula for the success probability.

The paper is organized as follows. In Sec. II we briefly describe the algorithm. The algebraic analysis is presented in Sec. III for the general case that involves several marked states with an arbitrary pure state as the initial state. Special cases such as the case of a single marked state are considered in Sec. IV. The generalization to mixed initial states is presented in Sec. V. The results are summarized in Sec. VI. The detailed calculation of the success probability of the algorithm is given in the Appendix.

II. THE QUANTUM SEARCH ALGORITHM

Consider a search space D containing N elements. We assume, for convenience, that $N = 2^n$, where n is an integer. The elements of D are represented using an n-qubit *register* containing the indices, $i = 0, \ldots, N-1$. We assume that a subset of r elements in the search space are marked, that is, they are solutions of the search problem. The distinction between the marked and unmarked elements can be expressed by a suitable function, $f : D \to \{0, 1\}$, such that $f = 1$ for the marked elements, and $f = 0$ for the rest. The search for a marked element now becomes a search for an element for which $f = 1$. To solve this problem on a classical computer one needs to evaluate f for each

element, one by one, until a marked state is found. Thus, on average, $N/2$ evaluations of f are required and N in the worst case. For a quantum computer, on which f to be evaluated *coherently*, it was shown that a sequence of unitary operations called Grover's algorithm can locate a marked element using only $O(\sqrt{N/r})$ coherent queries of f [1, 2].

To describe the operation of the quantum search algorithm we first introduce a register, $|i\rangle = |i_1 \dots i_n\rangle$, of n qubits, and an *ancilla* qubit, $|q\rangle$, to be used in the computation. We also introduce a *quantum oracle*, a unitary operator $\hat{O}$, which has the ability to *recognize* solutions to the search problem. The oracle performs the following unitary operation on computational basis states of the register, $|i\rangle$, and the ancilla, $|q\rangle$:

$$\hat{O}\,|i\rangle\,|q\rangle = |i\rangle\,|q \oplus f(i)\rangle \tag{1}$$

where $\oplus$ denotes addition modulo 2. The oracle recognizes marked states in the sense that if $|i\rangle$ is a marked element of the search space, namely $f(i) = 1$, the oracle flips the ancilla qubit from $|0\rangle$ to $|1\rangle$ and vice versa, while for unmarked states the ancilla is unchanged. The ancilla qubit is initially set to the state $|-\rangle_q = (|0\rangle - |1\rangle)/\sqrt{2}$. With this choice, the action of the oracle is $\hat{O}|i\rangle|-\rangle_q = (-1)^{f(i)}|i\rangle|-\rangle_q$. Thus, the only effect of the oracle is to apply a phase of -1 if x is a marked basis state, and no phase change if x is unmarked. The state of the ancilla does not change.

Grover's search algorithm may be described as follows: Given an oracle $\hat{O}$, whose action is defined by Eq. (1) and $n+1$ qubits in the state $|0\rangle^{\otimes n}|0\rangle_q$, the following procedure is performed:

1. Initialization: Apply a Hadamard gate $\hat{W} = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ to each qubit in the register, and the gate $\hat{W}\hat{X}$ to the ancilla, where $\hat{X} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ is the NOT gate, and we write matrices with respect to the computational basis $(|0\rangle, |1\rangle)$. The resulting state is $|\eta\rangle|-\rangle_q$, where

$$|\eta\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle. \tag{2}$$

2. Grover Iterations: Repeat the following operation τ times (where τ is given below).

   (a) Apply the oracle, which has the effect of rotating the marked states by a phase of π radians. Since the ancilla is always in the state $|-\rangle_q$ the effect of this operation may be described by the unitary operator $\hat{I}_M = \hat{I} - 2\sum_{m\in M} |m\rangle\langle m|$, acting only on the register, where $\hat{I}$ is the identity operator.

   (b) (i) apply the Hadamard gate on each qubit in the register; (ii) apply the operator $\hat{I}_0 = \hat{I} - 2|0\rangle\langle 0|$ which rotates the $|00\dots0\rangle$ state of the register by a phase of π radians. (iii) Apply the Hadamard gate again on each qubit in the register.

   The resulting operation is $-\hat{W}\hat{I}_0\hat{W} = -\hat{I} + 2|\eta\rangle\langle\eta|$. When this operator is applied on the state $\sum_i a_i|i\rangle$ it results in the state $\sum_i(2\bar{a} - a_i)|i\rangle$, where $\bar{a} = \sum_i a_i/N$. Thus, each amplitude is rotated by π around the average of all amplitides of the quantum state.

3. Measure the register in the computational basis.

The combined operation on the register in one Grover iteration is given by $\hat{Q} = -\hat{W}\hat{I}_0\hat{W}\hat{I}_M$. The optimal number of iterations before the measurement is

$$\tau = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{r}} \right\rfloor, \tag{3}$$

where $\lfloor x \rfloor$ is the largest integer which is smaller than x [2, 3, 13]. Moreover, at this optimal time a marked state can be found with almost certainty, or more precisely with probability $P_{\rm s} = 1 - O\left(1/\sqrt{N}\right)$. With this performance, Grover's algorithm was found to be optimal in the sense that it is as efficient as theoretically possible [4]. Note that the probability $P_s \approx 1$ can be achieved only for specific initial states such as the one produced in step 1 of the algorithm above. If this initial state is replaced by an arbitrary quantum state, the probability of succes, $P_{\rm s}$, is reduced [19, 20].

The time evolution of the amplitudes of the marked and unmarked states during Grover's iterations was studied in Ref. [20] for an arbitrary pure initial state $|\psi\rangle$. In particular, the optimal number of iterations and the success

probability were calculated, and found to depend on the specific choice of the set of marked states. Obviously, in a search process, the marked states are not known. Thus, the success probability should be averaged over all possible choices of the set of r marked states [22]. The results are that for any initial state $|\psi\rangle$ the optimal number of iterations is given by Eq. (3). The success probability, P_s can be expressed in terms of the average of all amplitudes of the state $|\psi\rangle$. In the next Section we introduce the algebraic approach to the analysis of Grover's search algorithm.

III. ALGEBRAIC ANALYSIS OF THE QUANTUM SEARCH PROCESS

Consider a search using Grover's algorithm, for one of r marked states in a space of $N = 2^n$ computational basis states, where n is the number of qubits in the register. The initial state is

$$|\psi\rangle = \sum_{i=0}^{N-1} a_i |i\rangle \tag{4}$$

where a_i is the amplitude of the basis state $|i\rangle$. Denote the set of indices of the marked states by $\mathcal{M}$. The amplitudes of the marked states will thus be a_m, $m \in \mathcal{M}$. The complementary set, of unmarked states is denoted by $\mathcal{U}$, namely the amplitudes of the unmarked states are a_u, $u \in \mathcal{U}$. Thus, for a given choice of the set of marked states, the initial state $|\psi\rangle$ can be expressed by

$$|\psi\rangle = \sum_{m\in\mathcal{M}} a_m |m\rangle + \sum_{u\in\mathcal{U}} a_u |u\rangle. \tag{5}$$

The amplitudes a_m and a_u satisfy:

$$\sum_{m\in\mathcal{M}} |a_m|^2 + \sum_{u\in\mathcal{U}} |a_u|^2 = 1. \tag{6}$$

Their averages are given by

$$\bar{a}_M = \frac{1}{r} \sum_{m\in\mathcal{M}} a_m \tag{7}$$

for the marked states, and

$$\bar{a}_U = \frac{1}{N-r} \sum_{u\in\mathcal{U}} a_u \tag{8}$$

for the unmarked states.

A. Construction of a four-dimensional subspace

The initial state $|\psi\rangle$ can be projected onto the subspaces spanned by the marked and unmarked basis states, giving rise to the normalized projections

$$|\phi_M\rangle = \frac{1}{\sqrt{P_0}} \sum_{m\in\mathcal{M}} a_m |m\rangle \tag{9}$$

and

$$|\phi_U\rangle = \frac{1}{\sqrt{1-P_0}} \sum_{u\in\mathcal{U}} a_u |u\rangle, \tag{10}$$

respectively, where

$$P_0 = \sum_{m\in\mathcal{M}} |a_m|^2. \tag{11}$$

The state $|\psi\rangle$ can now be written in the form

$$|\psi\rangle = \sqrt{P_0}|\phi_M\rangle + \sqrt{1-P_0}|\phi_U\rangle, \tag{12}$$

where $|\phi_M\rangle$ and $|\phi_U\rangle$ are orthogonal to each other. Similarly, the equal superposition state $|\eta\rangle$, can be expressed in the form

$$|\eta\rangle = \sqrt{\frac{r}{N}}|\eta_M\rangle + \sqrt{1-\frac{r}{N}}|\eta_U\rangle, \tag{13}$$

where

$$|\eta_M\rangle = \frac{1}{\sqrt{r}} \sum_{m\in\mathcal{M}} |m\rangle \tag{14}$$

and

$$|\eta_U\rangle = \frac{1}{\sqrt{N-r}} \sum_{u\in\mathcal{U}} |u\rangle. \tag{15}$$

From now on we will refer to the plane spanned by $|\eta_M\rangle$ and $|\eta_U\rangle$ as the *Grover plane*. Using the Gram-Schmidt procedure we extract from $|\phi_M\rangle$ and $|\phi_U\rangle$ two new states $|\psi_M\rangle$ and $|\psi_U\rangle$, that are perpendicular to $|\eta_M\rangle$ and $|\eta_U\rangle$. These states are given by

$$|\psi_M\rangle = \frac{|\phi_M\rangle - \langle\eta_M|\phi_M\rangle|\eta_M\rangle}{\sqrt{1-|\langle\eta_M|\phi_M\rangle|^2}} \tag{16}$$

and

$$|\psi_U\rangle = \frac{|\phi_U\rangle - \langle\eta_U|\phi_U\rangle|\eta_U\rangle}{\sqrt{1-|\langle\eta_U|\phi_U\rangle|^2}}. \tag{17}$$

Using the fact that

$$\begin{aligned} \langle\eta_M|\phi_M\rangle &= \sqrt{\frac{r}{P_0}}\bar{a}_M \\ \langle\eta_U|\phi_U\rangle &= \sqrt{\frac{N-r}{1-P_0}}\bar{a}_U, \end{aligned} \tag{18}$$

we can write $|\psi_M\rangle$ and $|\psi_U\rangle$ more explicitly as

$$\begin{aligned} |\psi_M\rangle &= \frac{\left(\sqrt{P_0}|\phi_M\rangle - \sqrt{r}\bar{a}_M|\eta_M\rangle\right)}{\sqrt{P_0 - r|\bar{a}_M|^2}} \\ |\psi_U\rangle &= \frac{\left(\sqrt{1-P_0}|\phi_U\rangle - \sqrt{N-r}\bar{a}_U|\eta_U\rangle\right)}{\sqrt{1-P_0-(N-r)|\bar{a}_U|^2}}. \end{aligned} \tag{19}$$

Thus, Eq. (12) now takes the form

$$|\psi\rangle = \sqrt{P_0 - r|\bar{a}_M|^2}|\psi_M\rangle + \sqrt{1 - P_0 - (N-r)|\bar{a}_U|^2}|\psi_U\rangle + \sqrt{N-r}\bar{a}_U|\eta_U\rangle + \sqrt{r}\bar{a}_M|\eta_M\rangle, \tag{20}$$

where the state vectors $|\psi_M\rangle$, $|\psi_U\rangle$, $|\eta_U\rangle$ and $|\eta_M\rangle$ define a set of four orthonormal basis vectors. In particular, $|\psi_M\rangle$ and $|\eta_M\rangle$ span the subspace of marked states, while $|\psi_U\rangle$ and $|\eta_U\rangle$ span the subspace of unmarked states. Also, $|\psi_M\rangle$ and $|\psi_U\rangle$ are perpendicular to $|\eta\rangle$. We will show below that for any initial state $|\psi\rangle$, iterations of the quantum search always preserve the subspace spanned by these four vectors.

B. The time evolution of the state vector

Denoting the Grover iteration by $\hat{Q}$, the state of the register after t iterations is

$$|g(t)\rangle = \hat{Q}^t|\psi\rangle. \tag{21}$$

Using the structure of the operator $\hat{Q}$ presented above, we obtain that for any state $|\psi\rangle$

$$\hat{Q}|\psi\rangle = -|\psi\rangle + 2\left(\langle\eta|\psi\rangle - 2\sum_{m\in\mathcal{M}}\langle\eta|m\rangle\langle m|\psi\rangle\right)|\eta\rangle + 2\sum_{m\in\mathcal{M}}\langle m|\psi\rangle|m\rangle. \tag{22}$$

Applying $\hat{Q}$ on the vectors that span the four-dimensional subspace we obtain

$$\begin{aligned}
\hat{Q}|\psi_M\rangle &= |\psi_M\rangle \\
\hat{Q}|\psi_U\rangle &= -|\psi_U\rangle \\
\hat{Q}|\eta_U\rangle &= \left(1 - \frac{2r}{N}\right)|\eta_U\rangle + 2\sqrt{\frac{r}{N}\left(1-\frac{r}{N}\right)}|\eta_M\rangle \\
\hat{Q}|\eta_M\rangle &= -2\sqrt{\frac{r}{N}\left(1-\frac{r}{N}\right)}|\eta_U\rangle + \left(1 - \frac{2r}{N}\right)|\eta_M\rangle.
\end{aligned} \tag{23}$$

The Grover iteration $\hat{Q}$ acts as a linear transformation within a four dimensional vector space, spanned by $|\psi_M\rangle$, $|\psi_U\rangle$, $|\eta_U\rangle$ and $|\eta_M\rangle$. For the analysis presented below it is convenient to use the vector representation

$$|\psi_M\rangle \equiv \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \qquad |\psi_U\rangle \equiv \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \qquad |\eta_U\rangle \equiv \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \qquad |\eta_M\rangle \equiv \begin{pmatrix}0\\0\\0\\1\end{pmatrix}, \tag{24}$$

in which, according to Eq. (20)

$$|\psi\rangle \equiv \begin{pmatrix} \sqrt{P_0 - r|\bar{a}_M|^2} \\ \sqrt{1 - P_0 - (N-r)|\bar{a}_U|^2} \\ \sqrt{N-r}\bar{a}_U \\ \sqrt{r}\bar{a}_M \end{pmatrix}. \tag{25}$$

The matrix representation of $\hat{Q}$ is:

$$\hat{Q} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & \cos\omega & -\sin\omega \\ 0 & 0 & \sin\omega & \cos\omega \end{pmatrix} \tag{26}$$

where

$$\cos\omega = 1 - \frac{2r}{N} \tag{27}$$

and

$$\sin\omega = 2\sqrt{\frac{r}{N}\left(1-\frac{r}{N}\right)}. \tag{28}$$

Therefore,

$$\hat{Q}^t = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & (-1)^t & 0 & 0 \\ 0 & 0 & \cos(\omega t) & -\sin(\omega t) \\ 0 & 0 & \sin(\omega t) & \cos(\omega t) \end{pmatrix} \tag{29}$$

and the state of the register after t iterations is

$$\begin{aligned} |g(t)\rangle \;=\; & \sqrt{P_0 - r|\bar{a}_M|^2}\;|\psi_M\rangle + (-1)^t\sqrt{1-P_0-(N-r)|\bar{a}_U|^2}\;|\psi_U\rangle \\ & + \left(\sqrt{N-r}\bar{a}_U\cos(\omega t) - \sqrt{r}\bar{a}_M\sin(\omega t)\right)|\eta_U\rangle \\ & + \left(\sqrt{N-r}\bar{a}_U\sin(\omega t) + \sqrt{r}\bar{a}_M\cos(\omega t)\right)|\eta_M\rangle. \end{aligned} \tag{30}$$

The four dimensional space in which the dynamics is confined includes the *plane of marked states*, spanned by $|\psi_M\rangle$ and $|\eta_M\rangle$ as well as the *plane of unmarked states* spanned by $|\psi_U\rangle$ and $|\eta_U\rangle$.

C. The success probability

The probability of success $P_s(t)$ of a measurement taken after t iterations is given by the projection of $|g(t)\rangle$ on the plane of marked states:

$$\begin{aligned} P_s(t) \;=\; & P_0 + \frac{1}{2}\left[(N-r)|\bar{a}_U|^2 - r|\bar{a}_M|^2\right] \\ & -\frac{1}{2}\left[(N-r)|\bar{a}_U|^2 - r|\bar{a}_M|^2\right]\cos(2\omega t) \\ & +\frac{1}{2}\sqrt{r(N-r)}(\bar{a}_U^*\bar{a}_M + \bar{a}_M^*\bar{a}_U)\sin(2\omega t). \end{aligned} \tag{31}$$

From Eq. (30) it is easy to see that $|g(t)\rangle$ exhibits a rotation with angular velocity ω in the *Grover plane* spanned by $|\eta_U\rangle$ and $|\eta_M\rangle$. This rotation causes an exchange of probability between the planes of marked and unmarked states. Thus, the success probability is limited by the projection of the initial state $|\psi\rangle$ on the Grover plane. The projection of $|\psi\rangle$ along $|\psi_U\rangle$, which is perpendicular to the Grover plane, represents a lost probability that cannot be transformed into the plane of the marked states. This provides an upper bound on the success probability $P_s(t)$, of the form

$$P_{\max} = P_0 + (N-r)|\bar{a}_U|^2. \tag{32}$$

Similarly, a lower bound on the success probability

$$P_{\min} = P_0 - r|\bar{a}_M|^2 \tag{33}$$

can be obtained using the projection in the direction of $|\psi_M\rangle$. Furthermore, by using the explicit forms of the states that span the four dimensional subspace and Eq. (30), the following expression for the temporal evolution of the state vector is obtained

$$|g(t)\rangle = \sum_{m\in\mathcal{M}} \left(\bar{k}(t) + \Delta a_m\right)|m\rangle + \sum_{u\in\mathcal{U}} \left(\bar{l}(t) + (-1)^t \Delta a_u\right)|u\rangle. \tag{34}$$

The variables

$$\bar{k}(t) = \sqrt{\frac{N-r}{r}}\ \bar{a}_U \sin(\omega t) + \bar{a}_M \cos(\omega t) \tag{35}$$

and

$$\bar{l}(t) = \bar{a}_U \cos(\omega t) - \sqrt{\frac{r}{N-r}}\bar{a}_M \sin(\omega t) \tag{36}$$

are the average amplitudes, after t iterations, of the marked and unmarked states, respectively. Also,

$$\begin{aligned} \Delta a_m &= a_m - \bar{a}_M, \quad m \in \mathcal{M} \\ \Delta a_u &= a_u - \bar{a}_U, \quad u \in \mathcal{U} \end{aligned} \tag{37}$$

represent the initial deviations of the amplitudes a_m and a_u from the averages of the marked and unmarked amplitudes, respectively [20].

The analysis presented above applies to any specific choice of the set of marked state. In practice, the set of marked states is not known. Thus, the success probability of an actual search is the average of $P_s(t)$ over all possible choices of the set of r marked states. In the limit of a large search space, where $r \ll N$, it takes the form (see Appendix):

$$\langle P_s(t)\rangle = N|\bar{a}|^2 \sin^2[\omega(t+1/2)] + O\left(r/N\right), \tag{38}$$

where

$$\bar{a} = \frac{1}{N}\sum_{i=0}^{N-1} a_i \tag{39}$$

is the average over all the amplitudes of the initial state $|\psi\rangle$. The optimal number of iterations, τ, is given by Eq. (3), namely, is identical to that obtained for the original algorithm. The probability of success of a measurement taken after τ iterations is

$$P_{\max} = N|\bar{a}|^2 + O\left(r/N\right). \tag{40}$$

It can also be expressed by $P_{\max} = |\langle\eta|\psi\rangle|^2 + O(r/N)$ [22].

IV. ANALYSIS OF SPECIAL CASES

Below we consider special cases in which the analysis can be simplified and the dimension of the subspace in which the Grover iterations operate is reduced.

A. Quantum search with a single marked state

Consider the quantum search algorithm with an initial state $|\psi\rangle$ and a single marked state $|m\rangle$. In this case the subspace of the marked states is one dimensional. Therefore, the normalized projection of the equal superposition state $|\eta\rangle$ on the subspace of marked states is given by

$$|\eta_M\rangle = |m\rangle. \tag{41}$$

Since the one dimensional subspace of the marked states does not include any perpendicular direction $|\psi_M\rangle = 0$. The average amplitude of the marked states is $\bar{a}_M = a_m$, where a_m is the amplitude of the marked state $|m\rangle$ in the initial state $|\psi\rangle$. Thus, the state $|g(t)\rangle$ of the register after t Grover iterations [Eq. (30)] takes the form

$$\begin{aligned} |g(t)\rangle &= \left(\sqrt{N-1}\bar{a}_U \cos(\omega t) - a_m \sin(\omega t)\right)|\eta_U\rangle + \left(\sqrt{N-1}\bar{a}_U \sin(\omega t) + a_m \cos(\omega t)\right)|m\rangle \\ &\quad +(-1)^t \sqrt{1-(N-1)|\bar{a}_U|^2 - |a_m|^2}\;|\psi_U\rangle. \end{aligned} \tag{42}$$

Clearly, $|g(t)\rangle$ is confined to the three dimensional subspace spanned by $|\eta_U\rangle$, $|m\rangle$ and $|\psi_U\rangle$.

In case that all the amplitudes a_i are real, the dynamics of the quantum search can be viewed as a rotation of the state vector $|g(t)\rangle$ around the bases of a cylinder, jumping from one base to the other at each time step. The axis of the cylinder is in the direction of $|\psi_U\rangle$. Its bases are in the Grover plane, namely spanned by $|\eta_U\rangle$ and $|m\rangle$. The radius of the cylinder is given by the projection of $|g(t)\rangle$ on the Grover plane:

$$R = \sqrt{(N-1)|\bar{a}_U|^2 + |a_m|^2}. \tag{43}$$

The length of the cylinder is twice the size of the projection of $|g(t)\rangle$ in the direction of $|\psi_U\rangle$, namely

$$L = 2\sqrt{1-R^2}. \tag{44}$$

The dynamics of the quantum search consists of rotations of the state vector $|g(t)\rangle$ around the $|\psi_U\rangle$ axis, at an angular velocity ω, combined with switching positions between the two bases. At even time steps $|g(t)\rangle$ points towards the upper base, while at odd times it points towards the lower base. The optimal measurement time is when the vector $|g(t)\rangle$ is exactly above (or below) the $|m\rangle$ axis.

B. Quantum search with an initial state in the Grover plane

Consider a quantum search with a certain set of r marked states, such that the initial state $|\psi\rangle$ is in the Grover plane. In this case $|\psi\rangle$ can be represented by

$$|\psi\rangle = \alpha|\eta_U\rangle + \beta|\eta_M\rangle \tag{45}$$

where α and β are complex amplitudes that satisfy $|\alpha|^2 + |\beta|^2 = 1$. Note that $|\psi\rangle$ has no component perpendicular to the Grover plane either in the subspace of marked states or in the subspace of unmarked states. Therefore, $|\psi_M\rangle = |\psi_U\rangle = 0$. The average amplitudes of the marked and unmarked basis states in $|\psi\rangle$ are $\bar{a}_M = \beta/\sqrt{r}$ and $\bar{a}_U = \alpha/\sqrt{N-r}$, respectively. The state vector after t iterations takes the form

$$|g(t)\rangle = [\alpha\cos(\omega t) - \beta\sin(\omega t)]\,|\eta_U\rangle + [\alpha\sin(\omega t) + \beta\cos(\omega t)]\,|\eta_M\rangle, \tag{46}$$

namely, it is confined to the Grover plane, where it rotates with angular velocity ω. The success probability $P_s(t)$ oscillates periodically between $P_{\min} = 0$ and $P_{\max} = 1$, namely the algorithm is optimal. For example, the equal superposition state $|\eta\rangle$ is a special case within this category, where $\alpha = \sqrt{N-r/N}$ and $\beta = \sqrt{r/N}$.

C. Quantum search with an initial state perpendicular to the Grover plane

Consider an initial state $|\psi\rangle$ which is perpendicular to the Grover plane, namely a state that satisfies $\langle\eta_M|\psi\rangle = \langle\eta_U|\psi\rangle = 0$. In this case $\bar{a}_M = \bar{a}_U = 0$ and

$$|g(t)\rangle = \sqrt{P_0}|\psi_M\rangle + (-1)^t\sqrt{1-P_0}|\psi_U\rangle. \tag{47}$$

This state vector is confined to a cycle of period 2, namely $|g(t+2)\rangle = |g(t)\rangle$. Recall that Grover's algorithm generates a flow of probability from the subspace of unmarked states toward the subspace of marked states only within the Grover plane. In this case $|\psi\rangle$ is perpendicular to the Grover plane. Therefore, the probability of success remains unchanged, namely $P_s(t) = P_0$, making the quantum search process useless. Two special cases can be identified. In case that $\bar{a}_U = 0$ and $a_m = 0$ for all $m \in M$, the success probability $P_s(t) = 0$ at any time t. In the opposite case where $\bar{a}_M = 0$ and $a_u = 0$ for all $u \in \mathcal{U}$, $P_s(t) = 1$ at all times.

V. QUANTUM SEARCH USING MIXED STATES

The quantum search with an initial state which is a mixed state was studied before for a specific choice of the set of marked states [21]. Here we extend the analysis to the general case in which the set of marked states is unknown and calculate the success probability. We first analyze the case of a genral mixed states and then discuss some special cases.

A. General analysis for arbitrary mixed states

Consider a quantum search using the mixed state

$$\hat{\rho}_0 = \sum_\mu p_\mu |\psi_\mu\rangle\langle\psi_\mu| \tag{48}$$

of n qubits as the initial state of the register. In this representation p_μ is the probability that corresponds to the pure state $|\psi_\mu\rangle$ in the ensemble and $\sum_\mu p_\mu = 1$. The pure states take the form

$$|\psi_\mu\rangle = \sum_{i=0}^{N-1} a_{\mu i}|i\rangle. \tag{49}$$

The average amplitude in the state $|\psi_\mu\rangle$ is

$$\bar{a}_\mu = \frac{1}{N}\sum_{i=0}^{N-1} a_{\mu i}. \tag{50}$$

The density operator after t iterations is given by

$$\hat{\rho}(t) = \hat{Q}^t\hat{\rho}_0\hat{Q}^{t\dagger} = \sum_\mu p_\mu |g_\mu(t)\rangle\langle g_\mu(t)| \tag{51}$$

where $|g_\mu(t)\rangle = \hat{Q}^t|\psi_\mu\rangle$. The measurement of the register in the computational basis is represented by the operator:

$$\hat{M} = \sum_{i=0}^{N-1} i\hat{M}_i, \tag{52}$$

where $\hat{M}_i = |i\rangle\langle i|$ is the measurement operator that corresponds to the outcome i. The success probability of a measurement taken after t iterations is

$$P_s(t) = \sum_{m\in\mathcal{M}} \mathrm{Tr}\left(\hat{M}_m^\dagger \hat{M}_m \hat{\rho}(t)\right) = \sum_\mu p_\mu P_s(\psi_\mu, t) \tag{53}$$

where

$$P_s(\psi_\mu, t) = \sum_{m\in\mathcal{M}} |\langle m|g_\mu(t)\rangle|^2. \tag{54}$$

Averaging the probability of success over all possible choices of the set of r marked states, where $r \ll N$, gives

$$\langle P_s(t)\rangle = N|\bar{a}|^2 \sin^2\left[\omega(t+1/2)\right] + O(r/N), \tag{55}$$

where

$$|\bar{a}|^2 = \sum_\mu p_\mu |\bar{a}_\mu|^2. \tag{56}$$

Thus, the maximal success probability

$$P_{\max} = N|\bar{a}|^2 + O(r/N) \tag{57}$$

is simply the weighted average of the success probabilities obtained using the pure states $|\psi\rangle_\mu$ as initial states. Using Eq. (56) and the fact that $|\langle\eta|\psi_\mu\rangle|^2 = N|\bar{a}_\mu|^2$ we find that $P_{\max} = \langle\eta|\hat{\rho}_0|\eta\rangle$. This is, in fact, the square of the fidelity of $\hat{\rho}_0$ and $|\eta\rangle$, namely,

$$P_{\max} = F^2(|\eta\rangle, \hat{\rho}_0). \tag{58}$$

B. Search using only part of the qubits in the register

Consider a quantum register of $n+k$ qubits, which is in a pure state $|\psi\rangle$. Suppose that the qubits are divided between two parties such that Alice gets the first n qubits and Bob gets the rest of them. The state of the register can be expressed by

$$|\psi\rangle = \sum_{\mu=0}^{K-1}\sum_{i=0}^{N-1} b_{\mu i}|i\rangle_A|\mu\rangle_B \tag{59}$$

where the subsystem of Alice is spanned by the basis $|i\rangle_A$, $i = 0, 1, \ldots, N-1$, where $N = 2^n$, while the subsystem of Bob is spanned by $|\mu\rangle_B$, $\mu = 0, 1, \ldots, K-1$, where $K = 2^k$. The normalization condition is

$$\sum_{\mu=0}^{K-1}\sum_{i=0}^{N-1} |b_{\mu i}|^2 = 1 \tag{60}$$

and

$$\bar{b} = \frac{1}{NK}\sum_{\mu=0}^{K-1}\sum_{i=0}^{N-1} b_{\mu i} \tag{61}$$

is the average amplitude. Eq. (59) can be written in the form

$$|\psi\rangle = \sum_{\mu=0}^{K-1} c_\mu |\psi_\mu\rangle_A |\mu\rangle_B \tag{62}$$

where

$$\sum_{\mu=0}^{K-1} |c_\mu|^2 = 1. \tag{63}$$

The pure state $|\psi_\mu\rangle_A$ of party A, that corresponds to the computational basis state $|\mu\rangle_B$ of party B is given by

$$|\psi_\mu\rangle_A = \sum_{j=0}^{N-1} a_{\mu j} |j\rangle_A \tag{64}$$

where $b_{\mu i} = c_\mu a_{\mu i}$. This state satisfies the normalization condition

$$\sum_{i=0}^{N-1} |a_{\mu i}|^2 = 1 \tag{65}$$

and its average amplitude is

$$\bar{a}_\mu = \frac{1}{N} \sum_{i=0}^{N-1} a_{\mu i}. \tag{66}$$

The measurement statistics for Alice is given by the reduced density operator:

$$\hat{\rho}^A = \mathrm{Tr}_B |\psi\rangle\langle\psi| = \sum_{\mu=0}^{K-1} p_\mu |\psi_\mu\rangle_A \ {}_A\langle\psi_\mu| \tag{67}$$

where Tr_B is a trace over the state of Bob and $p_\mu = |c_\mu|^2$.

Consider a quantum search in a search space of size NK using the entire register of $n+k$ qubits in the state $|\psi\rangle$. The success probability is

$$P_{\max}^{\mathrm{AB}} = NK|\bar{b}|^2 = \frac{N}{K} \left| \sum_{\mu=0}^{K-1} c_\mu \bar{a}_\mu \right|^2 + O\left(\frac{r}{NK}\right). \tag{68}$$

Now, consider the case in which Alice performs a quantum search in a space of size N using her n qubits in the state $\hat{\rho}^A$. The success probability of Alice's search is

$$P_{\max}^{\mathrm{A}} = N \sum_{\mu=0}^{K-1} p_\mu |\bar{a}_\mu|^2 = N \sum_{\mu=0}^{K-1} |c_\mu \bar{a}_\mu|^2 + O(r/N). \tag{69}$$

Using the inequality $|\bar{x}|^2 \leq \overline{|x|^2}$, for a random variable x_k, where equality is obtained only if all the x_k's are equal, we find that $P_{\max}^A \geq P_{\max}^{AB}$. This means that for a register in an entangled state $|\psi\rangle$, reducing the search space increases the success probability. Equality is obtained only if there is no entanglement between the systems held by Alice and Bob, and Bob's system is in the equal superposition state $|\eta\rangle_B$. Thus, one can always add or remove unentangled qubits in the state $(|0\rangle + |1\rangle)/\sqrt{2}$ without changing $P_{\max}$. However, adding entangled qubits reduces $P_{\max}$ while removing such qubits increases it.

C. Search using an initial pseudo-pure state

Consider a search using an initial state which is a pseudo-pure state of n qubits

$$\rho_\epsilon = (1-\epsilon)\frac{I}{N} + \epsilon|\psi\rangle\langle\psi|, \tag{70}$$

where $\hat{I}$ is the N-dimensional unit matrix representing the maximally mixed state, $|\psi\rangle$ is a pure state and $0 < \epsilon < 1$. The maximally mixed state can be represented by

$$I = \frac{1}{N}\sum_{i=0}^{N-1}|i\rangle\langle i|, \tag{71}$$

while the pure state $|\psi\rangle = a_i|i\rangle$, has an average amplitude $\bar{a}_\psi$. Using Eq. (55) we find that

$$P_{\max} = \frac{1-\epsilon}{N} + \epsilon N|\bar{a}_\psi|^2 + O(\epsilon r/N). \tag{72}$$

Therefore, the success probability is simply reduced by a factor of ϵ vs. its value in the case that the initial state is the pure state $|\psi\rangle$.

VI. SUMMARY

We have introduced an algebraic approach to the analysis of Grover's quantum search algorithm with an arbitrary initial quantum state. This approach reveals the geometrical structure of the search space, which turns out to be a four dimensional subspace of the Hilbert space. This approach unifies and generalizes earlier results on the time evolution of the amplitudes during the search, the optimal number of iterations and the success probability. Furthermore, it enables a direct generalization to the case in which the initial state is a mixed state, providing an exact formula for the success probability.

APPENDIX A: THE AVERAGE SUCCESS PROBABILITY

The probability of success of the quantum search algorithm after t iterations, for a given choice of the set of r marked states is given by Eq. (31). Since the set of marked states is not known (although their number, r, is specified) the actual success probability is the average $\langle P_s(t)\rangle$ over all possible choices of the set of marked states:

$$\begin{aligned}\langle P_s(t)\rangle &= \langle P_0\rangle + \frac{1}{2}\left[(N-r)\langle|\bar{a}_U|^2\rangle - r\langle|\bar{a}_M|^2\rangle\right] \\ &\quad -\frac{1}{2}\left[(N-r)\langle|\bar{a}_U|^2\rangle - r\langle|\bar{a}_M|^2\rangle\right]\cos(2\omega t) \\ &\quad +\frac{1}{2}\sqrt{r(N-r)}\left(\langle\bar{a}_U^*\bar{a}_M\rangle + \langle\bar{a}_M^*\bar{a}_U\rangle\right)\sin(2\omega t).\end{aligned} \tag{A1}$$

We will now evaluate the averages $\langle P_0\rangle$, $\langle|\bar{a}_U|^2\rangle$, $\langle|\bar{a}_M|^2\rangle$ and $\langle\bar{a}_U^*\bar{a}_M\rangle$. The average $\bar{a}$ over all amplitudes in $|\psi\rangle$, satisfies the inequality $|\bar{a}|^2 \le 1/N$ where equality is obtained only for the equal superposition state $|\eta\rangle$. The average of P_0 over all possible choices of the r marked states is

$$\langle P_0\rangle = \langle\sum_{m\in\mathcal{M}}|a_m|^2\rangle = \frac{C_{r-1}^{N-1}}{C_r^N}\sum_{j=0}^{N-1}|a_j|^2 = \frac{r}{N}, \tag{A2}$$

where the binomial coefficient

$$C_r^N = \frac{N!}{(N-r)!r!} \tag{A3}$$

is the number of different sets of r objects that can be picked out of N distinguishable objects. The second moments of the amplitude distribution are

$$\begin{aligned}
\langle|\bar{a}_U|^2\rangle &= \frac{1}{(N-r)^2}\langle\sum_{u_1\in\mathcal{U}} a_{u_1}\sum_{u_2\in\mathcal{U}} {a_{u_2}}^*\rangle = |\bar{a}|^2 + O\left(1/N^2\right) \\
\langle|\bar{a}_M|^2\rangle &= |\bar{a}|^2\left(1-\frac{1}{r}\right)+\frac{1}{rN}+O\left(1/N^2\right) \\
\langle\bar{a}_U^*\bar{a}_M\rangle &= \frac{1}{r(N-r)}\langle\sum_{m\in\mathcal{M}} a_m\sum_{u\in\mathcal{U}} {a_u}^*\rangle = |\bar{a}|^2 + O\left(1/N^2\right) \\
\langle\bar{a}_M\bar{a}_U^*\rangle &= \langle\bar{a}_U^*\bar{a}_M\rangle^* = |\bar{a}|^2 + O\left(1/N^2\right). \qquad \text{(A4)}
\end{aligned}$$

Substitution of the above averages in Eq. (A1) yields

$$\langle P_s(t)\rangle = N|\bar{a}|^2\sin^2\left[\omega(t+1/2)\right]+\frac{r}{N}\left(1-N|\bar{a}|^2\right)+O\left(1/N\right), \qquad \text{(A5)}$$

In the limit of a large search space and $r \ll N$, the expression for the success probability is reduced to

$$\langle P_s(t)\rangle = N|\bar{a}|^2\sin^2[\omega(t+1/2)]+O\left(r/N\right). \qquad \text{(A6)}$$

---

[1] L.K. Grover, in *Proceedings of the Twenty-Eighth Annual Symposium on the Theory of Computing* (ACM Press, New York, 1996), p. 212.
[2] L.K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[3] C. Zalka, Phys. Rev. A **60**, 2746 (1999).
[4] C.H. Bennett, E. Bernstein, G. Brassard and U. Vazirani, SIAM J. Comp. **26**, 1510 (1997).
[5] L.K. Grover, Phys. Rev. Lett. **79**, 4709 (1997).
[6] L.K. Grover, Phys. Rev. Lett. **80**, 4329 (1998).
[7] B.M. Terhal and J.A. Smolin, Phys. Rev. A **58**, 1822 (1998).
[8] G. Brassard, P. Hoyer and A. Tapp, in *Automata Languages and Programming*, edited by K.G. Larsen, S. Skyum and G. Winskel (Springer-Verlag, Berlin, 1998), Vol. 1443, p. 820.
[9] N.J. Cerf, L.K. Grover and C.P. Williams, Phys. Rev. A **61**, 032303 (2000).
[10] L.K. Grover, Phys. Rev. Lett. **85**, 1334 (2000).
[11] A. Carlini and A. Hosoya, Phys. Lett. A. **280**, 114 (2001).
[12] M. Boyer, G. Brassard, P. Hoyer and A. Tapp, in *Proceedings of the fourth workshop on Physics and Computation* , edited by T. Toffoli, M. Biafore and J. Leao (New England Complex Systems Institute, Boston, 1996), p. 36.
[13] M. Boyer, G. Brassard, P. Hoyer and A. Tapp, Fortsch. der Phys. **46**, 493 (1998).
[14] L.K. Grover, Phys. Rev. Lett. **80**, 4329 (1998).
[15] R.M. Gingrich, C.P. Williams and N.J. Cerf, Phys. Rev. A **61**, 052313 (2000).
[16] E. Biham, O. Biham, D. Biron, M. Grassl, D.A. Lidar and D. Shapira , Phys. Rev. A **63**, 012310 (2001).
[17] G.L. Long, W.L. Zhang, Y.S. Li and L. Nui, Commun. Theor. Phys. **32**, 335 (1999).
[18] G.L. Long, Y.S. Li, W.L. Zhang and L. Nui, Phys. Lett. **A 262**, 27 (1999).
[19] D. Biron, O. Biham, E. Biham, M. Grassl and D.A. Lidar, Generalized Grover search algorithm for arbitrary initial amplitude distribution, Proceedings of the 1st NASA International Conference on Quantum Computing and Quantum Communications, Palm Springs, California, USA, February 17-20, 1998, Lecture Notes in Computer Science 1509, p. 140, Edited by C.P. Williams (Springer-Verlag, 1998). .
[20] E. Biham, O. Biham, D. Biron, M. Grassl and D.A. Lidar , Phys. Rev. A **60**, 2742 (1999).
[21] E. Biham and D. Kenigsberg, Phys. Rev. A **66**, 062301 (2002).
[22] O. Biham, D. Shapira and Y. Shimoni, Phys. Rev. A **68**, 022326 (2003).
[23] A. Miyake and M. Wadati, Phys. Rev. A **64**, 042317 (2001).
[24] O. Biham, M.A. Nielsen and T.J. Osborne, Phys. Rev. A **65**, 062312 (2002).
[25] Y. Shimoni, D. Shapira and O. Biham, Phys. Rev. A **69**, 062303 (2004).